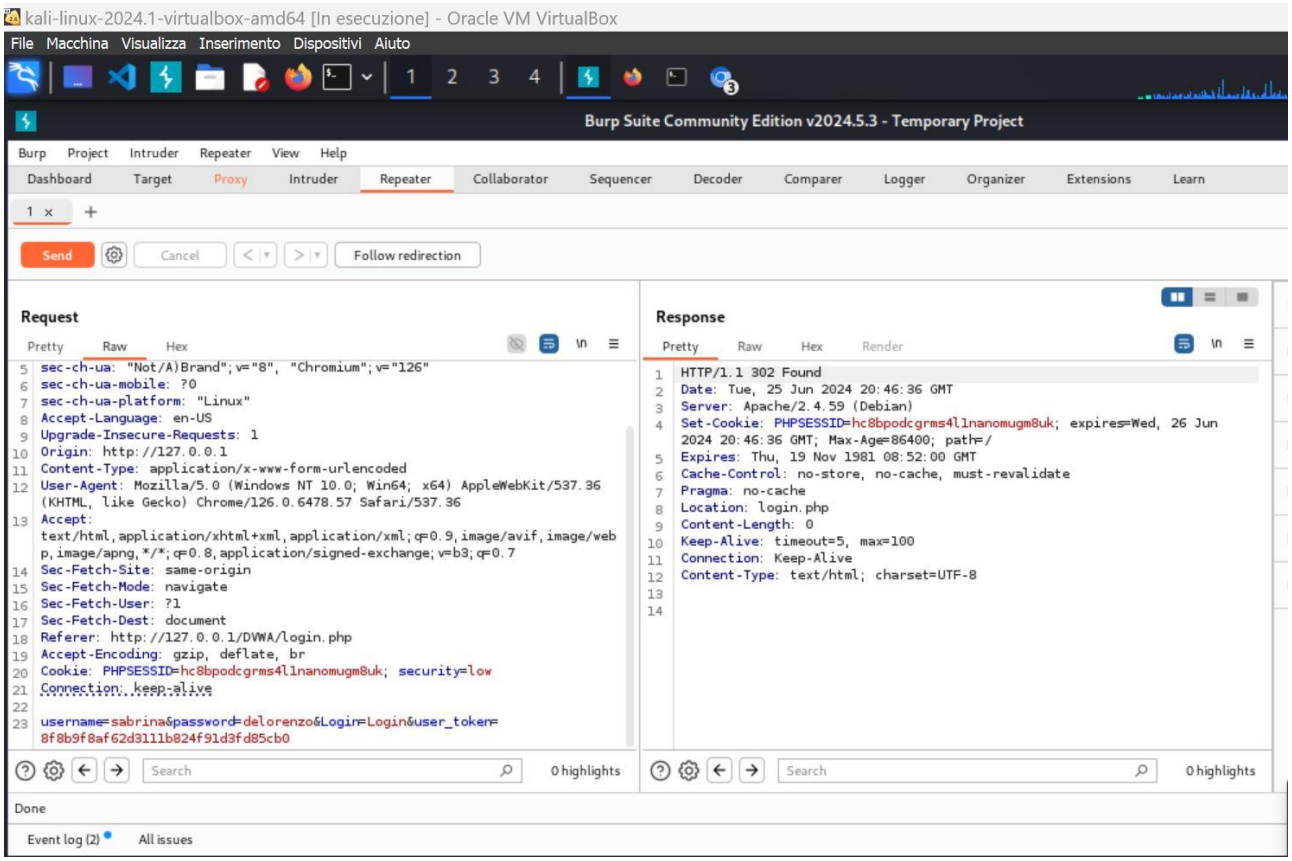
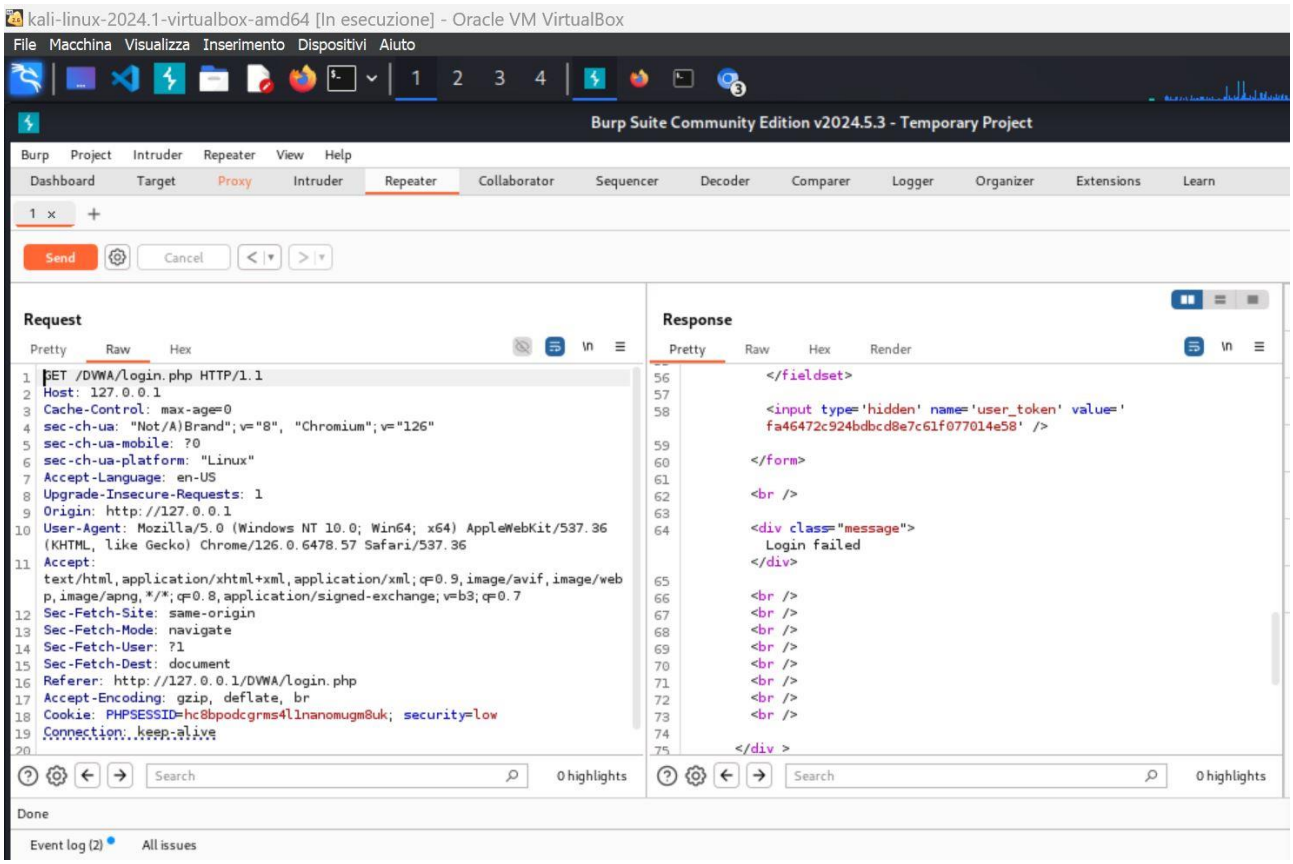
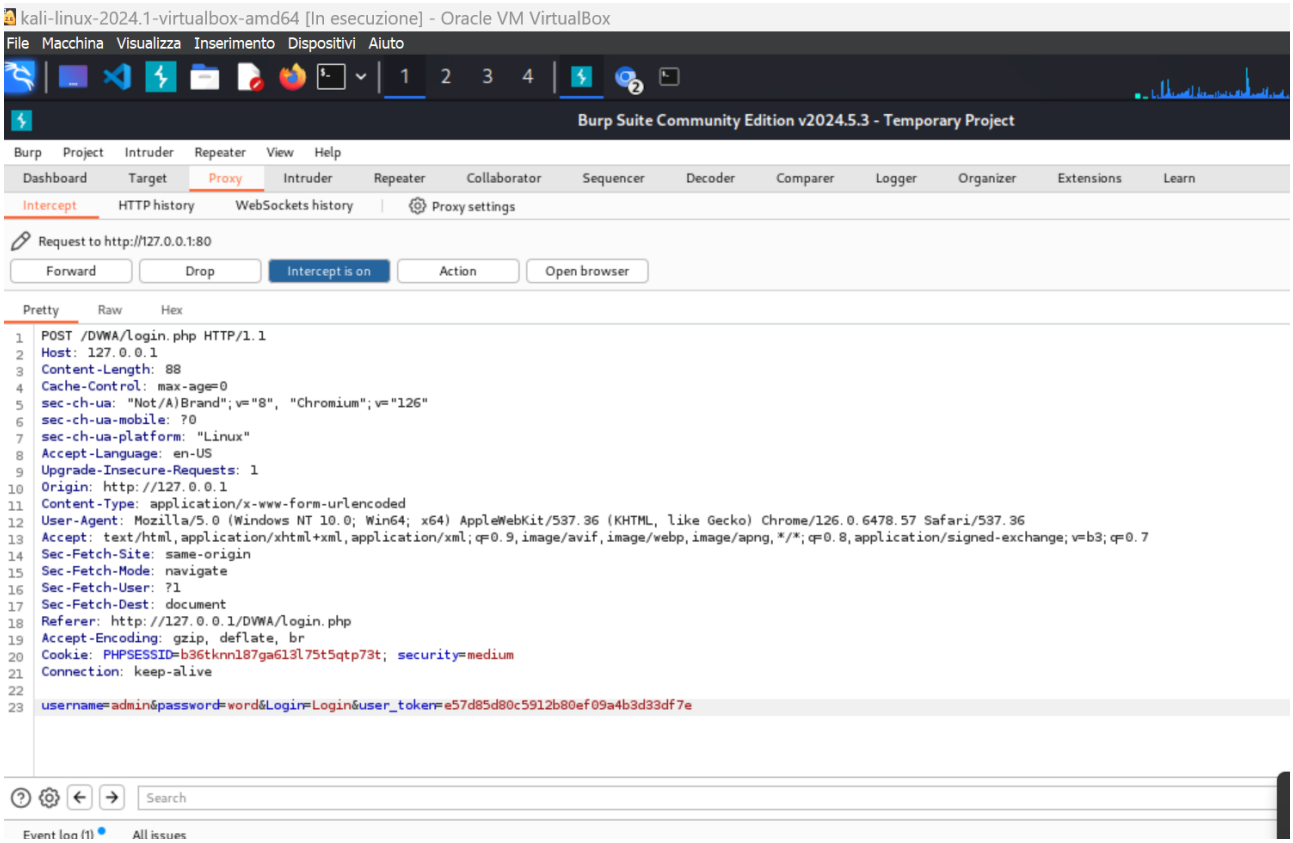
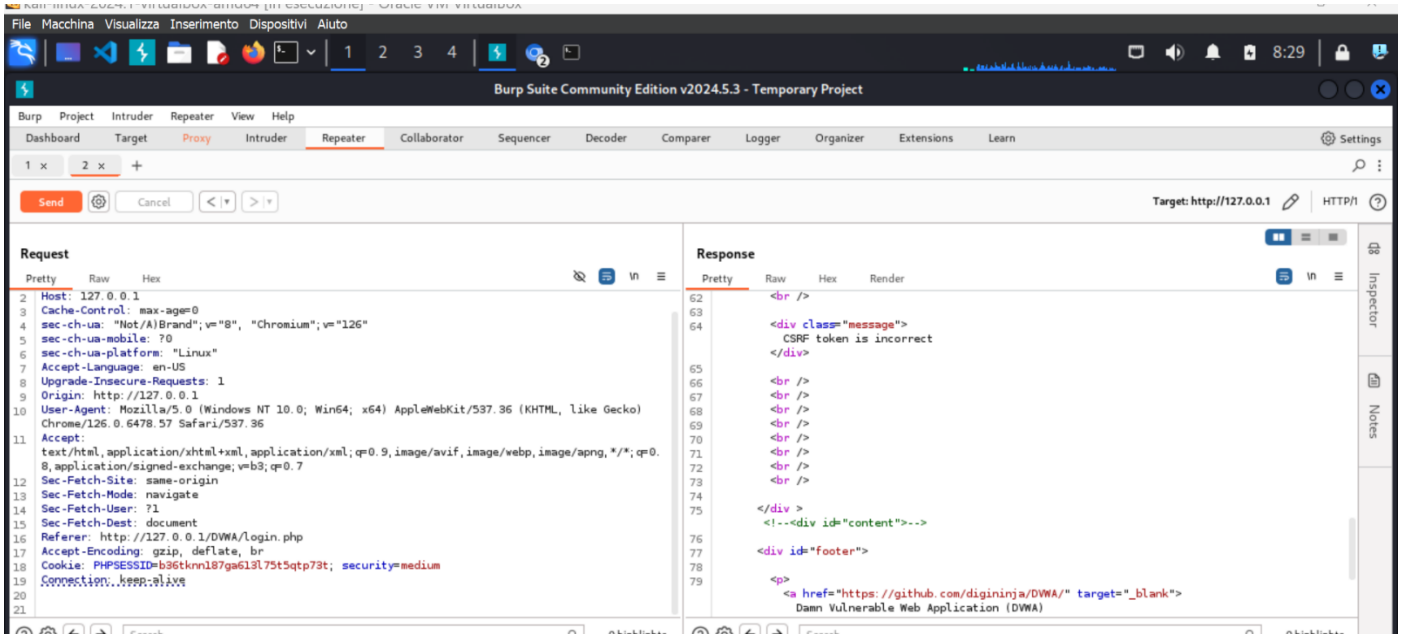
W8D1 + FACOLTATIVO





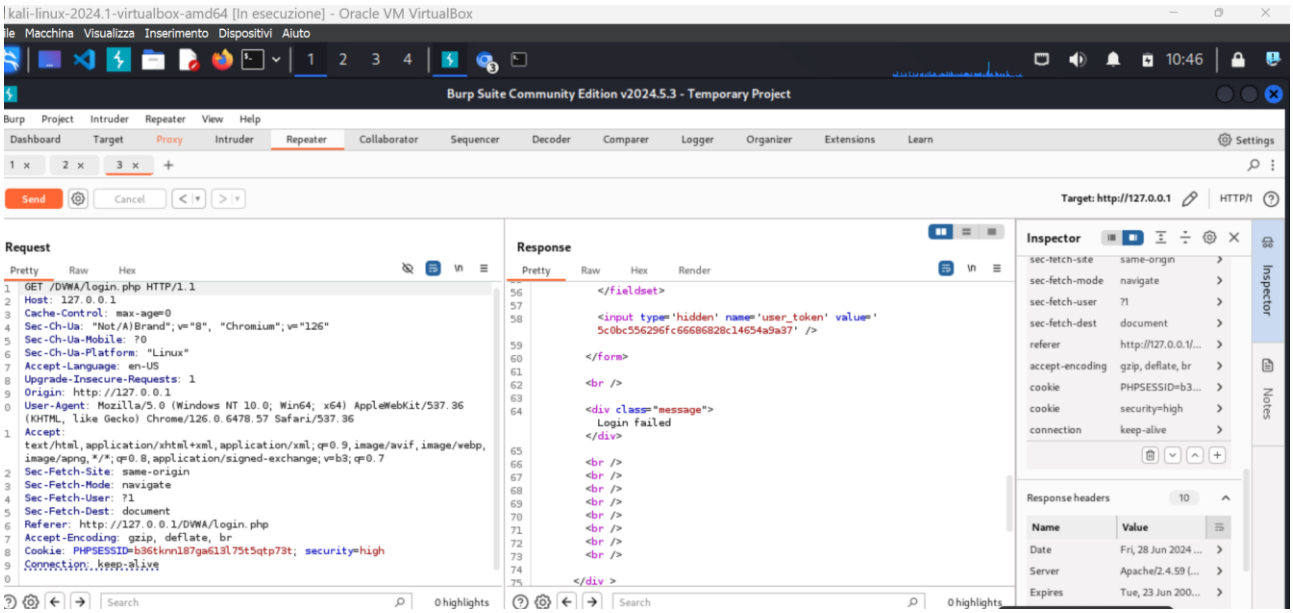

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=b36tknnl87ga613l75t5qtp73t; security=medium
Connection: keep-alive
username=admin&password=word&Login=Login&user_token=e57d85d80c5912b80ef09a4b3d33df7e
Search
Event log (1)
All issues


File Macchina Visualizza Inserimento Dispositivi Aiuto
Burp Suite Community Edition v2024.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: http://127.0.0.1
HTTP/1
Request
Pretty Raw Hex
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=b36tknnl87ga613l75t5qtp73t; security=medium
Connection: keep-alive
Response
Pretty Raw Hex Render

CSRF token is incorrect

<!--<div id="content">-->

<p>
<a href="https://github.com/digininja/DVWA/" target="_blank">
Damn Vulnerable Web Application (DVWA)
Inspector
Notes



Analisi delle Differenze tra i Livelli di Sicurezza

Livello di Sicurezza “Medium”

Con il livello di sicurezza impostato su "Medium", DVWA implementa alcune misure di sicurezza aggiuntive rispetto al livello "Low". Queste misure includono:

Convalida dei Dati:

Migliore convalida dei dati di input per prevenire SQL injection e altre forme di attacchi basati su input non sanitizzati.

Protezione contro CSRF:

Implementazione di token CSRF (Cross-Site Request Forgery) nei form per prevenire attacchi CSRF.

Protezione contro XSS:

Filtraggio dei caratteri speciali nei dati di input per prevenire attacchi di Cross-Site Scripting (XSS).

Livello di Sicurezza “High”

Con il livello di sicurezza impostato su "High", DVWA implementa misure di sicurezza ancora più rigorose. Queste misure potrebbero includere:

Hashing delle Password:

Utilizzo di hashing sicuro (come bcrypt) per proteggere le password memorizzate nel database.

Politiche di Sicurezza:

Implementazione di politiche di sicurezza più severe per la gestione delle sessioni e dei cookie.

Sanitizzazione Estesa:

Sanitizzazione estesa dei dati di input e output per prevenire una vasta gamma di vulnerabilità.

Confronto con il Livello “Low”

Login Bypass:

Con livello “Low”, potrebbe essere possibile bypassare il login tramite SQL injection modificando i parametri di login.

Con livello “Medium” o “High”, le misure di sicurezza aggiuntive rendono più difficile (se non impossibile) bypassare il login con semplici modifiche ai parametri.

Token CSRF:

A livello “Medium” e “High”, i form di login e altri form sensibili includeranno token CSRF, rendendo difficile inviare richieste fraudolente senza un token valido.

Hashing delle Password:

A livello “High”, le password memorizzate sono protette da hashing sicuro, rendendo inutili le tecniche di furto delle password come la semplice lettura del database.

L'intercettazione e la modifica delle richieste con Burp Suite su DVWA con i livelli di sicurezza "Medium" e "High" dimostrano l'importanza delle misure di sicurezza incrementali. Queste misure rendono più difficile sfruttare le vulnerabilità e proteggono meglio l'applicazione da attacchi comuni.